CLAIMS

What is claimed is:

1. A computerized method comprising:

monitoring a peer-to-peer network for suspicious activity based on patterns of activity; and

performing an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network.

2. The computerized method of claim 1, wherein monitoring a peer-to-peer network comprises:

evaluating network traffic among peers in the peer-to-peer network.

3. The computerized method of claim 1, wherein monitoring a peer-to-peer network comprises:

evaluating a change in shared data on a peer in the peer-to-peer network.

4. The computerized method of claim 1, wherein a pattern of activity is defined in terms of a threshold value of network traffic in the peer-to-peer network.

5. The computerized method of claim 1, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network that uses a specific protocol.

6. The computerized method of claim 1, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network that accesses shared data on a peer.

7. The computerized method of claim 1, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network having a foreign address.

8. The computerized method of claim 1, wherein a pattern of activity is defined in terms of a configuration of shared data on a peer.

9. The computerized method of claim 1, wherein the action comprises logging information about the particular pattern.

10. The computerized method of claim 1, wherein the action comprises sending an alert about the particular pattern.

11. The computerized method of claim 1, wherein the patterns of activity are local to a peer in the peer-to-peer network.

12. The computerized method of claim 1, wherein the patterns of activity are global to the peer-to-peer network.

13. The computerized method of claim 1 further comprising:

obtaining a set of rules specifying the patterns of activity and associated actions.

14. The computerized method of claim 13 further comprising:

refreshing the set of rules when the set of rules changes.

15. A computer-readable medium having executable instructions to cause a processor to perform a method comprising:

monitoring a peer-to-peer network for suspicious activity based on patterns of activity; and

performing an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network.

16. The computer-readable medium of claim 15, wherein the method further comprises:

evaluating network traffic among peers in the peer-to-peer network when monitoring the peer-to-peer network.

17. The computer-readable medium of claim 15, wherein the method further comprises:

evaluating a change in shared data on a peer in the peer-to-peer network when monitoring the peer-to-peer network.

18. The computer-readable medium of claim 15, wherein a pattern of activity is defined in terms of a threshold value of network traffic in the peer-to-peer network.

19. The computer-readable medium of claim 15, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network that uses a specific protocol.

20. The computer-readable medium of claim 15, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network that accesses shared data on a peer.

21. The computer-readable medium of claim 15, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network having a foreign address.

22. The computer-readable medium of claim 15, wherein a pattern of activity is defined in terms of a configuration of shared data on a peer.

23. The computer-readable medium of claim 15, wherein the action comprises logging information about the particular pattern.

24. The computer-readable medium of claim 15, wherein the action comprises sending an alert about the particular pattern.

25. The computer-readable medium of claim 15, wherein the patterns of activity are local to a peer in the peer-to-peer network.

26. The computer-readable medium of claim 15, wherein the patterns of activity are global to the peer-to-peer network.

27. The computer-readable medium of claim 15, wherein the method further comprises:

obtaining a set of rules specifying the patterns of activity and associated actions.

28. The computer-readable medium of claim 27, wherein the method further comprises:

refreshing the set of rules when the set of rules changes.

29. A system comprising:

a processor coupled to a memory through a bus;

a network interface coupled to the processor through the bus and further operable to selectively couple to a peer-to-peer network; and

a peer-to-peer security process executed by the processor from the memory to cause the processor to monitor the peer-to-peer network for suspicious activity based on patterns of activity, and to perform an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network.

30. The system of claim 29, wherein peer-to-peer security process further causes the processor to evaluate network traffic between the peers in the peer-to-peer network when monitoring the peer-to-peer network.

31. The system of claim 29 further comprising a computer-readable medium coupled to the processor through the bus, and wherein the peer-to-peer security process further causes the processor to evaluate a change in shared data on the computer-readable medium when monitoring the peer-to-peer network.

32. The system of claim 29, wherein the peer-to-peer security process further causes the processor to monitor the peer-to-peer network for a pattern of activity defined in terms of a threshold value of network traffic in the peer-to-peer network.

33. The system of claim 29, wherein the peer-to-peer security process further causes the processor to monitor the peer-to-peer network for a pattern of activity defined in terms of network traffic in the peer-to-peer network that uses a specific protocol.

34. The system of claim 29, wherein the peer-to-peer security process further causes the processor to monitor the peer-to-peer network for a pattern of activity defined in terms of network traffic that accesses shared data on a peer.

35. The system of claim 29, wherein the peer-to-peer security process further causes the processor to monitor the peer-to-peer network for a pattern of activity defined in terms of network traffic having a foreign address.

36. The system of claim 29 further comprising a computer-readable medium coupled to the processor through the bus, and wherein the peer-to-peer security process further

causes the processor to monitor the peer-to-peer network for a pattern of activity defined in terms of a configuration of shared data on the computer-readable medium.

37. The system of claim 29, wherein the peer-to-peer security process further causes the processor to log information about the particular pattern when performing the action associated with the particular pattern.

38. The system of claim 29, wherein the peer-to-peer security process further causes the processor to send an alert about the particular pattern when performing the action associated with the particular pattern.

39. The system of claim 29, wherein the system is a peer in the peer-to-peer network and the patterns of activity are local to the system.

40. The system of claim 29, wherein the system is a server in the peer-to-peer network and the patterns of activity are global to the peer-to-peer network.

41. The system of claim 40, wherein the system is a border firewall.

42. The system of claim 40, wherein the system is a domain name server.

43. The system of claim 29, wherein the peer-to-peer security process further causes the processor to obtain a set of rules specifying the patterns of activity and associated actions.

44. The system of claim 43, wherein the peer-to-peer security process further causes the processor to refresh the set of rules when the set of rules changes.